space, with a part B thereof being encrypted. As seen, the AS sub-program decrypts part B and stores the result which size should be not equivalent to that of the encrypted copy, in 'part B decrypted'.

The AS sub-program then overwrites at the first location of 'part B encrypted' an instruction 'JUMP TO part B decrypted' and at the end of 'part B decrypted' appends an instruction 'JUMP TO part C'. In this way, the encrypted part of the software will not be executed and the decrypted part will be executed instead.

In the case of audio/visual multimedia software, the software will be decrypted a small part by a small part and each small part is decrypted at the time it is about to be utilized by a audio/visual program for causing audio/visual effect. In other words, that audio/visual program has to cause the AS sub-program to be executed in the manner as described above in item 1b, everytime it wants a decryption of a small part. Desirably, a newly decrypted small part will overwrite a previously decrypted one so that a whole copy of the decrypted software will not exist in RAM.

4) The Sub-program for authenticating user computer (AC sub-program).

The AC sub-program for authenticating a computer on which it runs as being a particular predetermined computer, and prevent use of protected software if the computer is not, and its operation is under control of the central program.

Specifically, when the central program is being installed in a harddisk of a user computer and executed, it will check an encrypted status information stored in itself and from which it knows this is the first time it being executed and will cause an initialization process to take place. In the initialization process, the central program sends to the central computer, as mentioned herein above in item 2, an encrypted identity of the rightful user of the central program, then the AC sub-program requests for an encrypted command from the central computer which will provide such an encrypted command, in the manner as described herein above in item 3i, if the rightful user has a valid account which is not closed.

Dirty Claims

(Only claims being amended shown)

1. (Seven Times Amendment) A method for protecting software from unauthorised use, comprising the steps of:

determining if identity means /information, is existing in a processing apparatus under control of a user ;

using a favourable result of said determination as a pre-condition for causing said processing apparatus to provide said user access to said software desired to be protected ;

wherein :

said identity means/information, if so existing, being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

access to said software desired to be protected is being provided without causing a said operation being performed and said identity means/information being specific to said rightful user(s) [and said software desired to be protected being licensed to said rightful user(s)] .

4. (Second Times Amendment) A method for protecting software from unauthorised use , as claimed in claim 1, wherein said operation being operation related to making payment from an account of said rightful user(s) , for obtaining a service/product.

6. (Third Times Amendment) A method for protecting software from unauthorised use, as claimed in claim 5, wherein further comprising the steps of:

[said processing apparatus having] storing an encrypted identity of [its rightful] a user in said processing apparatus ; and if [one] all of said protected programs stored in said processing apparatus has a valid user identity which being [not] consistent with the decryption result of said stored encrypted identity [of said processing apparatus], permitting use of said protected programs [will not be permitted] and [will be permitted] not permitting if otherwise .

7. (Sixth Times Amendment) A computer software product for protecting software publicly distributed against unauthorised use ;

said software product comprising :

identity program code for enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

authorising software effectively under the control of said rightful user(s) for, when executed, providing user access to said software desired to be protected, without causing a said operation being performed ;

a computer readable medium having said identity program code and said authorising software ;

wherein :

said identity program code and said authorising software are [contained] stored in said [software product] medium in such a manner that said authorising software is prevented from being copied therefrom individually; and the improvement resides in said protection basing on no specific hardware and/or software [specific to said rightful user(s)] other than said identity program code and said identity program code being specific to said rightful user(s) ;

[and said identity program code and said authorising software existing in a computer readable medium] .

9. (Third Times Amendment) A computer software product as claimed in claim 7, wherein said authorising software contains said identity program code therein and said computer readable medium being in form of data signal embodied in a carrier wave.

10. (Eighth Times Amendment) A computer software product for protecting other software against unauthorised use , comprising :

authorising program for, when being executed, causing a processing apparatus to provide [providing] user access to said software desired to be protected ;

a computer readable medium having said authorising program ;

wherein :

information specific to rightful user(s) of said software desired to be protected, exists in said authorising program as a part thereof ;

said existing information being capable of being used in enabling electronic commerce operation(s) for which said rightful user(s) has to be responsible, but not being usable by said processing apparatus for said electronic commerce purpose, when said authorising program being loaded on said processing apparatus as a part thereof, and access to said software desired to be protected is being provided without causing a said operation being performed ;

[said authorising program existing in a computer readable medium].

11. (Third Times Amendment) A computer software product as claimed in claim 10, wherein said operation being operation related to making payment from an account of said rightful user(s) and said computer readable medium being in form of data signal embodied in a carrier wave.

14. (Seven Times Amendment) A method for protecting software from unauthorised use , comprising the steps of :

authenticating identity information/means associated with a processing apparatus under control of a user ;

using a favourable result of said authentication as a pre-condition for causing said processing apparatus to provide said user access to said software desired to be protected ;

wherein said identity information/means existing in such a manner that said identity information/means being capable of being used in enabling electronic commerce operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity information/means being specific to said rightful user(s) [and said software desired to be protected being licensed to said rightful user(s)].

18. (Seven Times Amendment) A method for protecting software from unauthorised use, by restricting the use thereof to be under control of a single person, comprising a sub-method ; said sub-method comprising the steps of :

(a) establishing a communication between a processing apparatus, say, first processing apparatus and a remote electronic transaction system ;

(b) verifying said person having a valid account, by said remote electronic transaction system, basing on authenticated information related to said person , said information being [obtained] communicated to said remote electronic transaction system from said processing apparatus ;

(c) using a favourable result of said verification as a pre-condition for [determining from said processing apparatus information related to the hardware or/and software thereof, for future reference in step (d) below ; thereafter]

(d) [authenticating a processing apparatus, say, second processing apparatus, basing on at least a part of said information related to said hardware or/and software ;]

(e) [using a favourable result of said authentication as a pre-condition for] permitting use of said software on said second processing apparatus, with no charge ;

wherein said sub-method a cost is being charged from said account ; and thereafter, said sub-method being capable of being used on a processing apparatus, say, third processing apparatus , without re-charging from said account said cost .

19. (Third Times Amendment) A method for protecting software from unauthorised use, as claimed by claim 18, wherein no charge [by said software distribution system] for repeating [at least] said sub-method [steps c] to e]] .

21. (Fourth Times Amendment) A method for verifying identity of a user of a data processing apparatus, comprising the steps of :

[a)] receiving, by said data processing apparatus, information specific to a user and necessary for accessing an account of said user ;

[b)] verifying said account being valid, by an electronic transaction system, by use of said information received by said data processing apparatus;

[c)] using by said data processing apparatus, a favourable result of said verification as a pre-condition for providing user access to at least a part of the functionality of said data processing apparatus ;

wherein said [steps a) to c) are] method is being performed without charging said account and said at least a part of functionality being not related to said validity status of said account.

22. (Second Times Amendment) A software product comprising computer code for causing one or more processing apparatus to perform the method of claim 1, 12, 14, 16, 18 , 20 or 21 ;

[said computer code existing in] a computer readable medium having said computer code.

23. A software product as claimed by claim 22, wherein said computer readable medium being in the form of data signal embodied in a carrier wave.